STATEMENT OF J. MICHAEL NETHERLAND

CYBERSMUGGLING INVESTIGATIONS DIVISION

BUREAU OF IMMIGRATION AND CUSTOMS ENFORCEMENT

HOUSE COMMITTEE ON GOVERNMENT REFORM

MARCH 13, 2003

I. INTRODUCTION:

Mr. Chairman and distinguished members of the Committee, it is a privilege to appear before you today to discuss the CyberSmuggling Center 's efforts to combat child exploitation that is facilitated by the Internet. The CyberSmuggling Center, led by the Bureau of Immigration and Customs Enforcement, will continue its proud history of combating the sexual exploitation of children and the unfettered accessibility and illegal bartering of child pornography on the Internet via peer-to-peer file sharing networks. The peer-to peer file sharing network is but one more means by which pedophile predators ply their trade and victimize our children and the CyberSmuggling Center is expanding its investigative efforts to encompass this new technology.

II. OVERVIEW

The CyberSmuggling Center, located in Fairfax, Virginia, is recognized both nationally and internationally as a leader in the area of child exploitation investigations. The CyberSmuggling Center utilizes its resources and cutting edge technology as a means to protect our nation's children from sexual abuse

and exploitation and has achieved great success in identifying and apprehending pedophiles. Recent investigative successes include:

- Operation HAMLET, a global investigation that resulted in the dismantlement of a ring of pedophiles who were molesting their own children and posting the images on the Internet for worldwide consumption. The CyberSmuggling Center, in its coordinative role, identified and rescued more than 100 children who were subjected to this torturous environment. The majority of these children were American citizens.
- Another example is Operation MANGO, which shut down an American-owned beachside resort for pedophiles located in Acapulco, Mexico. The resort was a haven for pedophiles that traveled to the facility for the sole purpose of engaging in sex with minors. As a result of this investigation and others, the government of Mexico recently created a federal task force to address crimes against children in its country.

The CyberSmuggling Center's technological capabilities include the National Child Victim Identification Program, a dynamic, one-of-a-kind information system that will eventually contain all known and unique child pornographic images. The primary goal of the program is to help law enforcement agencies throughout the world locate and rescue children who have been victimized for sexual purposes.

III. PEER-TO-PEER FILE SHARING NETWORKS

This Committee has asked that I address two specific concerns: (1) the ease of access and transmission of child pornography on peer-to-peer file sharing networks, and (2) the Bureau of Immigration and Customs Enforcement's efforts in tracking and investigating suspects that use this technology for criminal purposes.

A recent study undertaken jointly by the CyberSmuggling Center and the General Accounting Office (GAO) concluded that child pornography is easily accessed and transmitted via peer-to-peer file sharing networks. These networks are comprised of applications that allow subscribers to transfer various types of files, including image files, directly from one desktop to another in real time.

In its examination of peer-to-peer file sharing networks, the CyberSmuggling Center utilized twelve keyword search terms known by law enforcement to be associated with child pornography. Of the 1,286 files examined, forty-two percent (543) were determined to contain one or more images of child pornography. In another search utilizing just three keywords, nearly half of the files contained images classifiable as child pornography.

Keyword searches utilizing innocuous terms such as the names of cartoon characters and celebrities also produced multiple files containing child pornography. While the resulting percentages of illicit files were not nearly as high as for those generated using keywords typically associated with child

pornography, the study concluded that the threat of inadvertent exposure to Internet users, including juveniles, is significant.

Considering the fact that there are now more than twenty peer-to-peer software applications available on the Internet and that these applications are conducive to the unfettered transmission of images both legitimate and illegal, the CyberSmuggling Center has taken the position that peer-to-peer networks increase the likelihood of both intended and unintended exposure to child pornography.

The investigative efforts of the CyberSmuggling Center, while extensive and highly successful, have been geared to attack the problem of child exploitation on a reactive basis. This posture is dictated primarily as a result of the enormous volume of child pornography-related “tips” received and processed by the CyberSmuggling Center.

The CyberSmuggling Center handles more than 1,500 “tips” per month. Each “tip” requires an initial review resulting in a determination as to whether further investigation is warranted. If referred for investigation, then evidence must be gathered and a perpetrator identified. This is a time consuming, labor-intensive process. The majority of the CyberSmuggling Center’s resources are dedicated to “tip” response activities.

In contrast, the investigation of peer-to-peer networks can be classified as proactive in scope; i.e., investigators with no prior information can actively enter publicly accessible file sharing networks to detect illegal activity. Recognizing the potential use of peer-to-peer file sharing by pedophiles, the CyberSmuggling

Center reassigned an intelligence analyst to begin examining these types of cases in February 2002. To date, the CyberSmuggling Center has referred more than twenty leads to the field resulting in several successful enforcement actions including the arrest of a known child abuser.

Though we have only scratched the surface, peer-to-peer file sharing networks have received and will continue to receive increased scrutiny by the CyberSmuggling Center. Searches can be tailored to reveal images of child pornography, prosecutorial venue can be claimed at either end of the transaction, evidence is easily captured and preserved on a real-time basis, and violators are readily identifiable by investigators with the requisite training and experience. For these reasons, peer-to-peer file sharing investigations are likely to increase.

IV. CONCLUSION

In conclusion, let me reiterate that while we must, by necessity, continue to focus the majority of our attention and resources on the voluminous “tips” generated by outside entities, the CyberSmuggling Center will continue to expand its investigative efforts in the area of peer-to-peer file sharing.

I would like to thank the distinguished members of this committee for the opportunity to speak before you today and I welcome the opportunity to address any questions that you may have.